KURT GÖDEL: REVOLUCIÓN EN LOS FUNDAMENTOS DE LAS MATEMÁTICAS

ARBOR Ciencia, Pensamiento y Cultura
CLXXXIII 725 mayo-junio (2007) 409-418 ISSN: 0210-1963

Universidad de Sevilla

ABSTRACT: *We offer a survey of Kurt Gödel's main contributions in the field of Logic and foundations of mathematics, and we analyse their impact, which can well be called revolutionary. The aim is to contribute to an understanding of the aims and methodological orientation of Gödel's work, and to deal in some detail with their philosophical consequences. Thus, a perspective is offered on how the philosophy of mathematics changed between the dates of birth and death of this great mathematical logician.*

KEY WORDS: *Philosophy of mathematics, mathematical logic, foundations of mathematics, consistency, incompleteness, set theory, metamathematics, Hilbert's program, platonism.*

RESUMEN: Ofrecemos un repaso a las principales contribuciones de Kurt Gödel en el campo de Lógica y fundamentos de las matemáticas, analizando su impacto, que bien puede llamarse revolucionario. La pretensión es hacer comprensible la tendencia y orientación metodológica de los trabajos de Gödel, y considerar en algún detalle sus repercusiones filosóficas. Así, se ofrece una perspectiva de cómo cambió la filosofía de las matemáticas entre las fechas de nacimiento y muerte del genial lógico matemático.

PALABRAS CLAVE: Filosofía de las matemáticas, lógica matemática, fundamentos de las matemáticas, consistencia, incompletud, teoría de conjuntos, metamatemática, programa de Hilbert, platonismo.

El estudio de los fundamentos de la matemática es, desde hace un siglo, competencia de la Lógica Matemática. Se trata de un fenómeno bien característico del siglo XX: la propia matemática trata de dar cuenta de sus bases, convirtiéndose en una ciencia "reflexiva" que da lugar a la llamada *metamatemática*. Por usar la habitual metáfora de la ciencia en tanto edificio, es como si la arquitectura tratara de extender su campo de estudio para dar cuenta también de las bases geológicas en que tienen que asentarse, por necesidad, sus construcciones.

No hay duda de que la Lógica Matemática es una de las ramas matemáticas más propias del siglo XX, y más innovadoras (el otro gran ejemplo es la Topología). La lógica tiene una larga historia, que hunde sus raíces en la Antigüedad y la Edad Media, pero aquí nos referimos a la profunda renovación y transformación que produjo la interacción entre lógica y matemáticas en los años 1850-1940. El ascenso de la Lógica Matemática vino impulsado por cambios profundos en la concepción de las matemáticas, y a la vez su desarrollo en el siglo XX ha seguido generando cambios profundos. Es importante mencionar, asimismo, las innegables implicaciones que ha tenido la teoría lógica moderna a múltiples niveles: sobre todo el desarrollo de la computación, también en el campo de la lingüística, e incluso en filosofía dentro de la tradición analítica.

A grandes rasgos, cabe decir que la Lógica Matemática se descompone en las siguientes partes: (i) lógica elemental y sistemas formales; (ii) teoría de conjuntos; (iii) teoría de la computabilidad; (iv) teoría de la demostración; y (v) teoría de modelos. Pues bien, Gödel hizo aportaciones fundamentales a todos estos temas, aportaciones que fueron "directas al hueso", como se dice en inglés: atacando cuestiones verdaderamente clave y de implicaciones claras para los fundamentos de las matemáticas. Su obra dejó huella, pues esas aportaciones ayudaron a conformar las distintas ramas de la Lógica y reorientaron la discusión en su conjunto.

En 2006 se ha celebrado ampliamente el centenario de Kurt Gödel, quien, sin llegar a ser el mayor matemático del siglo XX, es indiscutidamente reconocido como el mayor lógico. Alfred Tarski, hombre ambicioso y quizá algo presuntuoso, llegó a comentar a un buen colega que se consideraba "the greatest living (sane) logician", con lo que evitaba –no muy sutilmente– el problema de su comparación con Gödel.

1. La situación hacia 1906

Al nacer Kurt Gödel, en abril de 1906, la comunidad matemática internacional se encontraba en plena discusión sobre las bases y las implicaciones de una serie de transformaciones fundamentales. Durante el XIX, la matemática había dejado de ser una "ciencia de las magnitudes", sus conceptos habían alcanzado un grado de abstracción sin precedentes, sus teorías se habían desarrollado mucho en extensión y profundidad, y al hacerlo surgía lo que hemos solido llamar "matemática moderna". Como muestra de lo que pretendo indicar, baste el siguiente ejemplo: en 1800, la idea de número real se consideraba un concepto científico impuesto por la realidad, por la presencia de magnitudes continuas en el mundo físico; en 1900, por contra, los números reales eran considerados producto del pensamiento puro, en tanto elementos de un conjunto dotado de la estructura de cuerpo ordenado arquimediano y completo. Estructura cifrada por Hilbert en 18 axiomas bastante simples, cuya mera *consistencia lógica* (la ausencia de contradicciones derivables lógicamente de esos 18 axiomas) era suficiente, en su opinión, para garantizar la *existencia* del conjunto de los reales.

La nueva matemática, impulsada especialmente desde Alemania por la escuela de Hilbert, se configuraba como un estudio de estructuras abstractas sobre la base de la axiomática y la teoría de conjuntos. Esta orientación suponía una ruptura respecto a la matemática del pasado, centrada en números, figuras y fórmulas: estos elementos tradicionales parecían "constructibles", generables paso a paso y resolubles paso a paso, al menos en principio, mientras que en torno a 1900 se hacía cada vez más claro el carácter "no constructivo" de la matemática moderna. Pero en el mismo momento en que la nueva tendencia parecía triunfar; cuando en el gran Congreso Internacional de París, 1900, el célebre Henri Poincaré la saludaba reconociendo que con ella se había alcanzado el rigor total; entonces surgían también dudas serias sobre la legitimidad de los métodos y los fundamentos postulados por la matemática moderna. Las dudas tuvieron sobre todo dos fuentes:

1. las paradojas de la teoría de conjuntos, descubiertas por Cantor hacia 1897 y desarrolladas por Russell: la paradoja de Burali-Forti o de la totalidad de los números ordinales transfinitos; la paradoja de Cantor o de la totalidad de los cardinales transfinitos; la paradoja de Zermelo-Russell o de la totalidad de los conjuntos que no son elementos de sí mismos; y otras muchas paradojas de naturaleza más lingüística o semántica;
2. los métodos de demostración basados en el axioma de elección, usados por Zermelo en 1904 para demostrar la "existencia" de un ordenamiento especial de los números reales (un *buen orden* sobre **R**) que nadie sabía cómo definir o "construir", esto es, cuya naturaleza "no constructiva" era tan evidente como para motivar una ola de críticas entre matemáticos franceses, alemanes y de otras naciones.

Consecuencia de este fermento de ideas fue un debate creciente sobre los fundamentos de las matemáticas, donde frente a los partidarios de la nueva matemática surgieron proponentes de enfoques más o menos rupturistas, liderados por algunos de los primeros espadas en matemáticas: el propio Poincaré, el intuicionista holandés Brouwer, o el alemán Weyl. Mientras Poincaré y Brouwer comenzaban a especificar qué postulados y métodos de la matemática conjuntista encontraban objetables, un colaborador de Hilbert, Ernst Zermelo, dedicaba su tiempo a formular un sistema simple de axiomas que fuera suficiente para edificar toda la teoría de conjuntos (sistema que incluía el polémico axioma de elección, pero a la vez excluía las paradojas de Burali-Forti, Cantor y Russell). Su sistema, llamado hoy de Zermelo-Fraenkel y denotado por las siglas *ZFC,* acabaría convirtiéndose en la axiomática más ampliamente aceptada como base para todo el edificio matemático.

En el desarrollo de las discusiones durante el primer tercio del XX, tres tendencias o "ismos" se dejaron notar especialmente:

1. el *logicismo,* surgido tiempo antes con Dedekind y Frege, luego revitalizado por Russell, quienes defendían que todos los conceptos y principios de las matemáticas pueden en último término reducirse a conceptos y leyes puramente lógicos;
2. el *formalismo,* que a grandes rasgos se identificaba con la posición de Hilbert: la matemática moderna se justifica por la posibilidad de axiomatizar con precisión sus principios, añadiendo la demostración rigurosa de que tales axiomas no llevan a contradicción (son *consistentes*);

ARBOR CLXXXIII 725 mayo-junio [2007] 409-418 ISSN: 0210-1963

3. y el *intuicionismo,* una creación matemática original de Brouwer, que rechazaba los métodos de la matemática moderna y los reemplazaba por métodos alternativos; métodos de elaboración más compleja, pero que parecían tener garantías especiales de evidencia y seguridad por basarse directamente en nuestras intuiciones del número y del continuo.

Frente al avance crítico de Brouwer y otros, el matemático más famoso de aquellos tiempos, David Hilbert, empeñó todo su prestigio en la promesa de ofrecer una demostración de consistencia para la aritmética y para la teoría de conjuntos. Se trataba de poner las bases de la nueva matemática más allá de toda duda razonable, al menos en cuanto a sus garantías lógicas:

> "eliminar de la faz de la tierra, de una vez y para siempre, las dudas escépticas sobre los fundamentos de las matemáticas",

como diría en 1927. En una conferencia "Sobre los problemas futuros de las matemáticas" impartida en el Congreso Internacional de 1900, que llegaría a hacerse legendaria, los dos primeros problemas eran sendas apuestas por el triunfo de la teoría de conjuntos y la axiomática: 1. "el problema cantoriano de la potencia del continuo"; 2. "la consistencia de los axiomas aritméticos". El propio Hilbert trató de resolver estos dos problemas con diversas aportaciones realizadas en 1905 y durante los años 1920, especialmente en su trabajo "Sobre el infinito" de 1925. Pero ninguno de sus tenaces intentos dio los frutos deseados. Sería precisamente Kurt Gödel, en 1931 y 1939, quien lograra avances definitivos en ambos frentes, y alguno de ellos en la dirección contraria a las esperanzas de Hilbert.

Desde 1905, los esfuerzos de Hilbert fueron en la dirección de aprovechar las posibilidades técnicas creadas por la Lógica Matemática, con la intención de realizar un estudio matemático de las propias teorías y demostraciones matemáticas. A esto llamó *metamatemática* o *teoría de la demostración:* el estudio de las posibilidades deductivas o demostrativas engendradas por un sistema axiomático dado posibilitaría, en su opinión, establecer el resultado negativo de que un sistema dado *no puede* dar contradicciones.

Históricamente, el avance de la lógica moderna se había iniciado con el desarrollo de nuevos cálculos "del razonamiento" (Boole, Frege, Peirce, Peano) y con el despliegue de la teoría de conjuntos en tanto elemento sistematizador y rigorizador del edificio matemático (Cantor, Dedekind, Zermelo, Russell). La fusión de ambas tendencias se produjo gradualmente en las primeras décadas del XX, bajo el impacto de los serios problemas que antes mencionamos: las paradojas conjuntistas y la llamada "crisis fundacional". Para resolver las paradojas y demás problemas se mostraba conveniente emplear los nuevos lenguajes lógicos, estrictamente regimentados y formalizados. Y esta conveniencia se tornó necesidad en el contexto del programa metamatemático de Hilbert, como veremos más abajo.

2. Lógica elemental

Cuando el joven Gödel comenzó sus estudios en la Universidad de Viena, años 1920, parece ser que su intención era dedicarse a la física. Sin embargo, el impacto de las lecciones sobre teoría de números del gran matemático Furtwängler le movió a cambiar dedicación, y su relación con miembros del famoso Círculo de Viena le puso en contacto con la lógica matemática de Russell. Teoría de números y lógica matemática: una combinación natural de suyo, pero que estaba llamada a alcanzar nuevas cotas de profundidad gracias a Gödel. Pronto Kurt se encontraba preparando la tesis doctoral bajo la dirección de Hans Hahn, matemático y miembro prominente del Círculo: su tema, resolver un problema planteado por Hilbert & Ackermann en sus *Grundzüge der theoretischen Logik* (*Fundamentos de lógica teórica,* Springer Verlag, 1928).

La consolidación definitiva de la Lógica Matemática, tal como hoy la entendemos, tuvo lugar en los años 1920 y 1930 bajo el impulso de Hilbert, Bernays y sus seguidores. El texto con el que Paul Bernays recogió y desarrolló las clases impartidas por Hilbert en el invierno de 1917/18, en Gotinga, puede considerarse el primer manual moderno de lógica matemática. Alcanzó la publicación unos años más tarde en los *Grundzüge* de Hilbert & Ackermann. La obra de Gödel se inscribiría plenamente en este contexto, y ha sido sin duda la más influyente contribución a la lógica de todo el siglo XX, que acabó por revolucionar el estudio de los fundamentos.

¿Por qué eran importantes los formalismos de la nueva lógica? Parte de la respuesta ha quedado ya indicada, pero falta decir qué los hacía imprescindibles para Hilbert. La idea clave de la nueva lógica matemática fue desarrollar un *lenguaje formal* perfectamente preciso con el que expresar los enunciados matemáticos, en particular los axiomas, y codificar *reglas de inferencia* que permitieran hacer totalmente precisas las demostraciones. Pensemos en la teoría de conjuntos: esta teoría, llevada a grandes alturas informalmente por Cantor y Dedekind, fue luego codificada y formalizada por Zermelo, Fraenkel, Skolem y otros. El axioma:

> Dado un conjunto C existe otro, $\wp$(C), cuyos elementos son todos los subconjuntos de C,

queda codificado por el enunciado formal:

$$\forall c \quad \exists d \quad \forall x \quad (x \in d \leftrightarrow x \subseteq c)$$

[que leemos: "Para todo *c* existe un *d* tal que para todo *x, x* pertenece a *d* si y sólo si *x* es subconjunto de c"; nótese que $d = \wp(c)$, y que el símbolo $\subseteq$ admite definición explícita en términos de $\in$]. Cuando todos los axiomas son formalizados, la teoría entera queda reducida a lo que llamamos un *sistema formal;* las deducciones dentro de la teoría se reducen a emplear única y exclusivamente las *reglas de inferencia,* son puramente formales. La teoría no es ya otra cosa que la totalidad de los enunciados (en el lenguaje formal que se ha estipulado con toda precisión) que son consecuencias lógicas de los axiomas.

Esta idea capital fue inventada por Frege hacia 1879, pero lo que para él era meramente una cautela metodológica al servicio de la filosofía, se convirtió con Hilbert en la clave para transformar problemas de fundamentos en problemas puramente matemáticos.

Hilbert venía defendiendo que el matemático sólo debe preocuparse de la *consistencia* o no-contradictoriedad de sus axiomas. Por supuesto, las ideas matemáticas tienen origen en la experiencia cotidiana, en la física, etc., pero con el tiempo los conceptos matemáticos son sometidos a crítica y las teorías son elevadas al estatus de puros entramados conceptuales. Llegados a este punto, estamos en el mundo abstracto de la matemática pura, y podemos afirmar la existencia de cualesquiera objetos, siempre que sus propiedades características y las relaciones entre estos objetos queden recogidas en un entramado conceptual –un sistema axiomático– que sea consistente. A fin de cuentas, para Hilbert la expresión "existe *x*", en matemáticas, apunta sólo a una *existencia ideal,* o si se quiere la admisibilidad del objeto *x* (caracterizado por ciertos axiomas) en un mundo de abstracciones lógico-conceptuales.

Supongamos que todo eso es correcto, y que por tanto basta con la simple consistencia lógica: la ausencia de toda contradicción en el plano rígidamente reglamentado de la teoría matemática, del sistema formal. El problema era: ¿cómo demostrar que las teorías interesantes son consistentes? La teoría de los números reales formulada por Dedekind y Hilbert, o la teoría de conjuntos codificada por Zermelo, tienen ya un grado de complejidad notable. Cualquier dominio de objetos (por muy "ideales" que sean) en el que se verifique una teoría u otra debe ser un dominio infinito bastante complejo. El sistema de Zermelo era fruto de una reflexión profunda, permitía trabajar libremente con conjuntos al tiempo que eliminaba las paradojas, pero ¿realmente lograba eliminar *toda* contradicción? Las matemáticas del infinito habían conducido a contradicciones difíciles de superar, tanto que algunos matemáticos muy influyentes habían apostado por el *finitismo* estricto: eliminar el infinito del universo conceptual de las matemáticas.

La idea crucial debió ocurrírsele a Hilbert en el transcurso de 1903, con motivo de reflexiones renovadas acerca de las dificultades que enfrentaba la teoría de conjuntos en tanto fundamento. Su intuición genial fue que la formalización de las matemáticas por medio de la lógica permitía tratar el problema de la consistencia como un problema matemático simple: mera cuestión de combinatoria finita, representable incluso como un problema de teoría de números. He aquí la manera. Cada teoría matemática, al ser formalizada, se reduce a un sistema finito de símbolos: todo teorema es el resultado de una *serie finita de inferencias* (reguladas por las reglas de inferencia) que en último término se originan en los axiomas, los cuales no son más que *secuencias finitas de símbolos.* La cuestión es, entonces, si la combinatoria finita de símbolos que es la teoría puede originar la demostración de una contradicción. Una contradicción no es más que una fórmula de la forma: $(p \wedge \neg p)$, y en el contexto de la lógica formal

basta incluso preguntarse si una contradicción concreta, una sola, es deducible (por ejemplo, si el sistema contiene símbolos para los números, basta saber si hay una deducción de la fórmula 0>1).

Estudiar las inferencias y deducciones formales en las teorías matemáticas formalizadas era, precisamente, el objetivo de la *teoría de la demostración* o *metamatemática* de Hilbert. Sería posible, así, analizar toda una serie de características de las teorías matemáticas. He aquí las principales:

– *independencia* o dependencia de los axiomas entre sí;
– *completud* de la teoría, esto es, si todos los enunciados relevantes (delimitados de manera sintáctica o semántica) son deducibles;
– *decidibilidad* de los enunciados, o sea, si existe un algoritmo que permita saber que un enunciado pertenece a cierto conjunto de ellos;
– y sobre todo el problema de la *consistencia,* cuya solución debía eliminar para siempre las dudas escépticas.

El programa se trató de desarrollar de manera progresiva, como era natural. Se esperaba dar primero una demostración de consistencia de la aritmética de Peano (el sistema axiomático para los números naturales), y más tarde proceder a establecer la consistencia de la aritmética de los números reales (con lo que quedaría fuera de dudas el análisis matemático). En el camino, se delimitó toda una serie de sistemas y se perfeccionaron los métodos de la lógica. Ya en las lecciones de 1917/18, mencionadas arriba, se caracterizaba con precisión lo que hoy llamamos la *lógica de primer orden.* En este sistema lógico, el más importante para las matemáticas y el estudio de sus fundamentos, contamos con símbolos para las conectivas lógicas 'y', 'o', 'no', 'si... entonces...', respectivamente:

$$\wedge,\ \vee,\ \neg,\ \rightarrow,$$

y para los cuantificadores 'para todo *x*', 'existe un *x*', respectivamente:

$$\forall x,\ \exists x.$$

Siendo el sistema puramente formal, los objetos en el dominio de los cuantificadores son individuos cualesquiera: no existen en lógica de primer orden recursos para "hablar" de "todas las propiedades". (Esto exigiría lógicas de segundo orden o de orden superior, las cuales presentan problemas en el contexto de los fundamentos de la matemática.)

Hilbert & Ackermann, en su obra citada (1928), planteaban el problema de demostrar que ese sistema lógico básico, la lógica cuantificacional o de primer orden, es *completo* en el sentido antes indicado. Este limitado pero importante problema fue el objeto de la tesis de Gödel, defendida en 1929. Pongamos que Σ es un conjunto cualquiera de fórmulas en el lenguaje de la lógica de primer orden (LPO). Gödel demostró que todas las consecuencias lógicas de Σ resultan demostrables a partir de las fórmulas de Σ mediante las reglas de inferencia de LPO. Para ello, Gödel estableció que todo conjunto (consistente) de fórmulas en el lenguaje LPO tiene un modelo enumerable en el sentido de la teoría de conjuntos (es decir: el modelo es finito o admite correspondencia uno-a-uno con los números naturales). De aquí se deducía otra consecuencia importante respecto a las propiedades de la LPO: el teorema de compacidad, que tendría gran importancia en el contexto de la teoría de modelos. Gödel obtuvo así un *metateorema lógico* que suele estudiarse en todo curso universitario de lógica matemática[1]. Pero lo mejor estaba por llegar.

3. Incompletud y teoría de la demostración

Demostrar la completud de la lógica de primer orden era un avance hacia la realización del programa que Hilbert se había marcado como objetivo de su metamatemática. Recordemos que se trataba de investigar varias propiedades de los sistemas formales: independencia de los axiomas, completud, decidibilidad, y consistencia. Hilbert asumía, de manera algo implícita o a veces indirecta, que no sólo LPO, sino también otros sistemas formales eran completos y consistentes: en particular, varios sistemas formalizados como el de los axiomas de Dedekind y Peano; el sistema de axiomas de los números reales; y el sistema axiomático *ZFC* de la teoría de conjuntos. Y obviamente, Hilbert suponía que los métodos empleados en metamatemática eran suficientes para demostrar que dichos sistemas son consistentes.

Gödel saltó a la fama con su enorme logro de 1931: la demostración del Primer Teorema de Incompletud, y la

idea de cómo demostrar un segundo teorema del que hablaremos más abajo. Tras anunciar los teoremas en varios lugares, Gödel los publicó en su obra "Sobre proposiciones formalmente indecidibles de los *Principia Mathematica* y sistemas afines", aparecida en la revista *Monatshefte für Mathematik und Physik*. Estos resultados de la metamatemática arruinaban buena parte de las esperanzas de Hilbert. No tendría sentido aquí intentar una descripción precisa del contenido y los métodos de ambos teoremas[2]. Nos limitaremos a dar una idea de su tendencia fundamental y de sus repercusiones.

Los sistemas formales definidos o codificados en la lógica de primer orden son, como hemos visto, de carácter finito y combinatorio. Cada enunciado es una secuencia finita de símbolos –por ejemplo: $\forall c \quad \exists d \quad \forall x \quad (x \in d \leftrightarrow x \subseteq c)$ – y hay algoritmos que determinan si una secuencia dada está bien formada o no. Cada demostración formal es una secuencia finita de fórmulas, que puede escribirse como varias líneas, en cada una de las cuales aparece una fórmula. Una nueva línea en la demostración se justifica pura y simplemente por las reglas de inferencia (formales o combinatorias) y por una o varias de las líneas que la preceden. Y hay algoritmos que determinan si una secuencia dada de fórmulas es o no es una demostración. En resumidas cuentas, al formalizar una teoría matemática en LPO, lo que estamos haciendo es reducir todo lo relativo a los enunciados de la teoría y sus demostraciones a un mero asunto de combinatoria de símbolos. Precisamente por ser consciente de esto, Hilbert se convenció de que era posible desarrollar una teoría matemática de las demostraciones formales.

Pensemos ahora en la teoría de números. Los números naturales son instrumentos que manejamos para representar todo tipo de fenómenos de carácter finito. Más aún, cualquier cuestión que sea sólo de carácter combinatorio y finito puede siempre ser reformulada como una cuestión acerca de números (Tait 1981). Esto no debería sorprendernos mucho, y hoy menos que nunca. Recuerdo al lector que, en el mundo digital que nos hemos creado, los números naturales nos permiten codificar todo tipo de informaciones: programas informáticos, por supuesto, y el contenido de cualquier libro, y gráficos, etc., pero también la cara de mi abuelo (tal como queda reflejada en una fotografía) y las melodías y armonías de la sinfonía 41 de Mozart tal como las interpretara von Karajan... ¡o la voz de Hilbert en el año 1930![3] Con más razón, y con mucha mayor precisión, pueden los números codificar todos los asuntos de combinatoria finita.

Tratemos ahora de reunir y combinar lo que acabamos de decir en los párrafos anteriores. Dado que cualquier sistema formal es de carácter combinatorio y finito, resulta posible establecer una representación o codificación de la información relevante sobre el sistema mediante números naturales. Es decir, podemos asignar números a los símbolos del sistema, y también a las fórmulas del sistema. Y lo más interesante: las relaciones entre las fórmulas se corresponderán también con relaciones bien definidas entre sus códigos numéricos. Esto es, lo relativo a la metamatemática del sistema es codificable en términos aritméticos. Semejante codificación digital del sistema formal y su metateoría se llama a veces una *gödelización,* y los números asignados se llaman "números de Gödel" (o incluso "gödels" a secas) de los signos, fórmulas, demostraciones, etc.

Una vez realizada esa codificación, es posible determinar efectivamente propiedades como si cierto número *n* es el número de un signo, o si es el número de Gödel de una fórmula. Dada una teoría T, hay algoritmos para determinar si cualquier fórmula dada es un axioma, si cierta ristra de fórmulas es una demostración formal, etc. Por tanto, es posible determinar efectivamente propiedades como las siguientes: si el número *n* es el número de Gödel de un axioma, o es el número de una demostración formal. Y también se puede determinar efectivamente la relación que se da entre los números *n* y *m* cuando *m* es el gödel de una demostración formal a partir de T de la fórmula cuyo gödel es *n.*

¿Por qué resulta todo esto interesante? Simple y llanamente, porque se trata de métodos muy fructíferos, y porque fue explotando las posibilidades de esas codificaciones (esa aritmetización de la metamatemática) como Kurt Gödel logró establecer sus llamativos resultados de 1931.

La teoría de los números naturales, en particular, puede ser axiomatizada y formalizada: se trata de la Aritmética de Dedekind-Peano (ADP). Pero aplicando el procedimiento de gödelización, se obtiene una representación del sistema formal ADP dentro de la propia aritmética; y por tanto, es posible representar el sistema y su metamatemática

dentro de sí mismo. Lo cual permitía, dando un nuevo giro a la reflexividad que está aquí involucrada, obtener un resultado capital. Gödel supo emplear las relaciones aritméticas para "cocinar" una fórmula φ que no puede ser demostrada ni refutada dentro del sistema formal, so pena de inconsistencia[4].

La fórmula φ de Gödel se obtiene considerando cuidadosamente la manera concreta en que se ha "gödelizado" el sistema formal, por ejemplo ADP. Conociendo el modo en que las propias relaciones aritméticas interpretan o codifican propiedades metamatemáticas, es posible interpretar φ como una afirmación de su propia indemostrabilidad[5]. La fórmula φ está construida de tal modo que, si φ fuera demostrable en el sistema formal, éste sería contradictorio; y si la negación de φ fuera demostrable, también sería contradictorio. Suponiendo pues que el sistema sea consistente (como creemos que lo es ADP y los demás sistemas que interesan a los matemáticos), la fórmula φ es *formalmente indecidible* dentro del propio sistema. Pero, como añadía el propio Gödel,

> De la observación que [φ] afirma su propia indemostrabilidad, se sigue inmediatamente que [φ] es correcta, puesto que [φ] es ciertamente indemostrable (pues es indecidible). Y así, la proposición que es indecidible *en el sistema* ***PM*** resulta con todo ser decidida por consideraciones metamatemáticas.

Aunque el sistema formal particular para el que Gödel demostró su Primer Teorema era el mencionado ***PM*** (basado en los *Principia Mathematica* de Whitehead y Russell), estaba claro que resultados análogos se podían demostrar para ADP o para sistemas como el *ZFC* de la teoría de conjuntos. En la descripción anterior no hemos entrado en detalles técnicos, pero como el lector podrá imaginar se ha establecido con toda precisión la clase de los sistemas afectados. Para la gödelización o aritmetización de la metateoría no hace falta ni siquiera disponer de toda la aritmética, es suficiente con una parte de ella (llamada aritmética recursiva primitiva). Cualquier sistema formal que tenga la capacidad expresiva suficiente para formular esa parte de la aritmética, está sujeto al Primer Teorema de Gödel. Esto sucede con la teoría de conjuntos o los sistemas formales para el análisis.

La existencia de un sistema formal incompleto no es en sí particularmente sorprendente. Un sistema puede ser incompleto simplemente porque no se han descubierto todos los axiomas necesarios. Lo que demostró Gödel es que, en casos de gran importancia como la aritmética o el análisis real, *nunca* se puede lograr un conjunto completo de axiomas. La incompletud es esencial: cada vez que se añada un nuevo axioma siempre habrá otra proposición que resulte indecidible.

4. Teoría de conjuntos

Según parece, Kurt Gödel tuvo siempre preferencia por la idea de que las matemáticas estudian un dominio de objetos, de *entidades independientes* cuya existencia y propiedades son objetivas. Parece ser que en su juventud limitaba esa actitud suya a los números naturales, mientras que consideraba como creaciones humanas a las ideas matemáticas más avanzadas (el concepto de conjunto, por ejemplo). Pero poco a poco su "platonismo" o realismo con respecto a los objetos matemáticos se fue ampliando, hasta incluir los conjuntos. En esto tuvieron un papel importante sus trabajos sobre la teoría de conjuntos y su metamatemática.

Las contribuciones de Gödel en este campo fueron muchas y de gran calado. Para empezar, la visión intuitiva de los conjuntos que hoy prefieren los especialistas (denominada la *concepción iterativa* de los conjuntos) fue aportación de Gödel en los años 1930 y 1940. Según esta concepción, comenzamos con un dominio limitado de objetos, por ejemplo los números naturales, y formamos *conjuntos de* esos objetos. Y la operación "conjunto de" puede *iterarse*, para formar conjuntos de conjuntos de conjuntos... Dicho proceso iterativo se concibe como abierto y absolutamente sin límites. La idea no está exenta de dificultades, pero ofrece una concepción sólida que justifica con relativa facilidad los axiomas habituales del sistema de Zermelo-Fraenkel, y aclara también por qué las famosas paradojas o contradicciones no afectan a la teoría axiomática de conjuntos.

Más importantes todavía fueron las contribuciones técnicas que Gödel realizó hacia 1940. Se trató de aplicar los métodos de la lógica matemática al estudio metateórico del sistema axiomático de Zermelo-Fraenkel (y otros sistemas alternativos de teoría de conjuntos). Suponiendo dado un modelo *M* del sistema de Zermelo-Fraenkel, Gödel

consideró un submodelo (en el interior de *M*) constituido por lo que se denominan *conjuntos constructibles.* Tales modelos internos resultaron tener propiedades de gran interés, permitiendo resolver varias dificultades.

Como vimos antes, desde comienzos de siglo venía existiendo una gran controversia en torno al Axioma de Elección. Con sus nuevos métodos, Gödel demostró en 1939 que, si la teoría de Zermelo-Fraenkel (sin Axioma de Elección) es consistente, entonces también lo es la teoría *ZFC* que añade a la anterior dicho axioma. Esto es así, porque dado un modelo del simple sistema Zermelo-Fraenkel, el modelo interno de conjuntos constructibles satisface a la teoría *ZFC.* Gracias a este resultado, las cautelas extraordinarias que se venían tomando en relación al Axioma de Elección perdieron base.

Análogamente, Gödel demostró que la Hipótesis del Continuo de Cantor puede añadirse a la teoría *ZFC* sin que afecte en absoluto a su consistencia. Pero Gödel creía que, en realidad, la Hipótesis de Cantor era independiente de los axiomas habituales, de modo que a fin de cuentas no era sino una *proposición indecidible* en la teoría de conjuntos estándar. Los trabajos de Paul Cohen en los años 1960, que introdujeron una nueva etapa en el desarrollo de la teoría de conjuntos (con su método de *forcing*) y le valieron la Medalla Fields, confirmaron plenamente esa idea.

Finalmente, nuestro hombre fue también el gran impulsor de lo que se llama a veces el "*Programa de Gödel*" en teoría de conjuntos, que encuentra su justificación en resultados como los anteriores y en el Teorema de Incompletud. La idea era avanzar hacia un mejor conocimiento del universo de los conjuntos introduciendo axiomas que establecen la existencia de lo que se llama "grandes cardinales" (con una modestia en la expresión que algunos califican de poética). Si la teoría de conjuntos estudia los cardinales infinitos, todos los cuales parecen enormes o incluso monstruosos a una persona media, los "grandes cardinales" son exorbitantemente grandes. Pero su estudio ha guiado buena parte de la labor de los especialistas durante el último medio siglo, produciendo resultados notables y de una sofisticación matemática muy considerable.

Sigue siendo un problema abierto si la introducción de grandes cardinales conducirá a resolver el Problema del Continuo de Cantor. Gödel creía, en realidad[6], que la hipótesis de Cantor es falsa, y que la cardinalidad del continuo es $\aleph_2$. Según importantes especialistas, hay resultados recientes que apuntan en esta misma dirección, pero todavía se está lejos de ninguna demostración fehaciente.

5. Repercusiones: el panorama en fundamentos

Según vimos, durante el primer tercio del siglo XX las principales corrientes, dentro del estudio de los fundamentos de la matemática, eran logicismo, formalismo e intuicionismo. Las aportaciones de Gödel afectaron profundamente a toda la discusión y contribuyeron quizá más que ninguna otra a modificar sus términos.

Cabría argumentar que el logicismo estaba ya en pleno retroceso antes de Gödel, pero en todo caso sus resultados afectaron a esta corriente del mismo modo que al formalismo. Ambas propugnaban la formalización completa de las teorías matemáticas, y presuponían ingenuamente que los nuevos sistemas formales (especialmente los de importancia práctica, como los sistemas para la aritmética y el análisis real) serían completos. El Primer Teorema de Incompletud de 1931 cayó no como un jarro, sino como una verdadera inmersión en agua fría, y sus consecuencias se sentirían por muchos años. Se sienten todavía, porque es un resultado inapelable que afecta a nuestra comprensión del conocimiento matemático. En mi opinión, contraria a lo que piensa algunos matemáticos, la conclusión principal es que no se puede identificar las matemáticas con una (o varias) teorías formales; pero esto tampoco nos arroja en brazos del platonismo.

Las teorías formales son instrumentos matemáticos de gran alcance y de gran interés. También interés práctico, ya que los desarrollos de la lógica matemática asociados al nombre de Gödel han conducido a las teorías de la computabilidad, constituyendo la base teórica del desarrollo de la tecnología de computadores. Pero las teorías formales son instrumentos que tienen límites severos: en los casos interesantes son incompletas, no sirven para caracterizar unívocamente el dominio de entidades que se pretende estudiar, etc. Gödel contribuyó más que ningún otro a aclarar esta situación.

La tendencia que se vio más afectada fue la formalista, y en particular el Programa de Hilbert para la demostración

de que las teorías matemáticas son consistentes. Gödel no sólo demostró el teorema del que hablamos en la sección 3, sino también un Segundo Teorema de Incompletud. Los procedimientos de gödelización o aritmetización hacen posible formular una fórmula *Con(S)* que codifica la consistencia del sistema formal *S,* y esto puede hacerse de tal modo que la fórmula φ que vimos en la sección 3 sea deducible de *Con(S).* Los detalles técnicos son delicados, de manera que la demostración de este Segundo Teorema es bastante más difícil que la del primero. Pero la consecuencia es clara: la fórmula *Con(S)* es también indecidible. La consistencia de un sistema formal de este tipo *no es demostrable sin emplear medios que no son codificables dentro del propio sistema.*

El Programa de Hilbert pretendía demostrar la consistencia de la aritmética ADP, de *ZFC,* y sistemas afines mediante *medios finitos.* Pero tales medios son codificables dentro de cualquiera de dichos sistemas. Gödel estableció pues que la meta que Hilbert se había fijado era inalcanzable. Por aclarar la situación metafóricamente, el intento de Hilbert quedó en una posición similar a los del barón de Münchhausen (personaje literario de Rudolf Erich Raspe): el barón había caído con su caballo en una ciénaga, e intentaba salir tirándose de su propia coleta. Igualmente fútiles parecían los intentos de resolver las dudas escépticas sobre las matemáticas con medios matemáticos.

En seguida, Gödel pasó a estudiar otros aspectos de los sistemas formales que tenían interés para la polémica entre formalistas e intuicionistas. Los intuicionistas, ya lo vimos, ponían objeciones a los métodos usuales en matemáticas, hasta el punto de rechazar incluso la forma normal de argumentar en aritmética. Así elaboraron una "aritmética intuicionista", y esta teoría acabó siendo formalizada en un sistema que llamaremos AI. Pues bien, en 1933 Gödel demostró que si el sistema AI es consistente, también lo es la aritmética "clásica" del sistema ADP. No era un resultado tremendo, pero cuestionaba las dudas de los intuicionistas. También sirvió para clarificar las ideas de los especialistas en fundamentos, que hasta entonces habían confundido los métodos finitarios con los métodos intuicionistas. Se entendía ahora, por fin, que los segundos van más allá de los primeros.

Tras todos estos giros, el panorama en fundamentos acabó mutando. El formalismo siguió estando fuerte a mediados del XX, aunque más como ideología conveniente que como una alternativa seria, ya que se había ido la esperanza de conseguir la clave de bóveda que debían haber constituido las demostraciones de consistencia. Hacia 1950, el logicismo había casi desaparecido, porque a las dificultades mostradas por Gödel se le unían otras específicas suyas. Entretanto, las peculiaridades de los métodos matemáticos, que la Lógica Matemática hizo tanto por clarificar, se convertían en argumentos plausibles a favor del platonismo. Y así, la tendencia preferida por Gödel se volvió una alternativa sólida en la práctica, aunque rodeada de dificultades filosófico-científicas[7].

El intuicionismo y, más en general, las posiciones denominadas constructivistas no desaparecieron, pero se consolidaron como una alternativa minoritaria. Así pues, y hablando a grandes rasgos, en la segunda mitad del siglo eran mayoritarias las posiciones que combinaban de modos diversos aspectos del formalismo y del platonismo[8]. Un triunfo más de Gödel.

La teoría de la demostración, por cierto, ha seguido desarrollándose con gran éxito. Téngase en cuenta que los propios teoremas de Gödel, por sorprendentes que fueran sus resultados, constituían grandes éxitos de los métodos metamatemáticos. Pero no ha resultado ser la panacea anunciada por Hilbert. Otra gran figura del siglo XX, John von Neumann, se había dedicado con ahínco al estudio de los fundamentos y al Programa de Hilbert. Tras los teoremas de Gödel, que von Neumann fue quizá el único en comprender inmediatamente, su desencanto con estos temas fue enorme. Decidió volverse hacia campos de las matemáticas que no fueran tan abstractos, sino que estuvieran en contacto directo con las ciencias, con la inyección vivificadora de ideas procedentes de la experiencia.

El desarrollo intelectual de Gödel fue en otra dirección. Continuó trabajando con intensidad en lógica matemática y fundamentos en las siguientes décadas. Pero, poco a poco, se fue centrando más en tratar de darle justificación filosófica a sus ideas preferidas. Se entregó así al estudio de textos filosóficos, a la reflexión sobre la obra de Leibniz y sobre la fenomenología de Husserl. Especuló con la posibilidad de elaborar una nueva ontología de los conceptos, y así fueron pasando los años, cada vez más recluido en el Institute for Advanced Study de Princeton. Continuaron la coherencia enorme y cierta tendencia a la obsesión que habían caracterizado su vida, y caracterizaron también su muerte por "desnutrición e inanición" en 1978.

NOTAS

1 Aunque a menudo se estudia en una versión posterior, debida al recién fallecido Leon Henkin en 1949.

2 Para esto, el lector consultará con provecho el trabajo de Jané (2006) que se cita en la bibliografía. Véase http://www.divulgamat.net/weborriak/Historia/Gaceta/Gaceta.asp

3 http://math.sfsu.edu/smith/Documents/HilbertRadio/HilbertRadio.mp3. Aquí habla Hilbert de que en matemáticas no hay problemas sin solución: "*debemos saber y sabremos*".

4 Digo "cocinar" porque la fórmula φ no tiene interés aritmético por sí misma. Otros lógicos han buscado fórmulas indecidibles más naturales, y la búsqueda continúa con H. Friedman.

5 Por eso se dice a menudo que hay cierta similitud entre el Primer Teorema de Incompletud de Gödel y la paradoja del mentiroso ("La frase que Ud. está leyendo, escrita entre paréntesis y comillas, es falsa").

6 Véase su artículo más fácil de leer: "¿Qué es el problema del continuo de Cantor?" (1947 y 1964), recogido en las *Obras completas*.

7 Para una discusión de este tema, puede verse Ferreirós (1999).

8 Hay más alternativas, claro, tanto por el lado filosófico como por el lógico-matemático: predicativismo, teoría de categorías, etc. Pero no podemos entrar en detalles.

Recibido: 16 de diciembre de 2006
Aceptado: 22 de diciembre de 2006

BIBLIOGRAFÍA

Escritos de Gödel

Obras completas, Alianza, Madrid, 1989.

"La situación presente en los fundamentos de las matemáticas", en *La Gaceta de la Real Sociedad Matemática Española,* vol. 9, 3, 2006, 761-771.

Collected Works. Volúmenes I-V. Ed. S. Feferman *et al.,* Oxford University Press, New York, 1986-2003.

Biografía

Dawson, John W. (1997): *Logical Dilemmas: The Life and Work of Kurt Gödel,* A. K. Peters, Wellesley (Mass.).

Análisis desde el punto de vista lógico y filosófico

Feferman, Solomon (1998): *In the Light of Logic,* Oxford University Press, New York, 1998.

Ferreirós, José (1999): "Matemáticas y platonismo(s)", en *La Gaceta de la Real Sociedad Matemática Española,* vol. 2, 446-473.

Franzén, Torkel (2005): *Gödel's Theorem. An Incomplete Guide to Its Use and Abuse,* A K Peters, Wellesley (Mass.).

Jané, Ignacio (2006): "La obra de Gödel en lógica matemática y teoría de conjuntos", en *La Gaceta de la Real Sociedad Matemática Española,* vol. 9, 3, 772-788.

Tait, W. (1981): "Finitism", *Journal of Philosophy,* 78; reimpreso en Tait, *The Provenance of Pure Reason,* Oxford University Press, 2005.

Wang, Hao (1991): *Reflexiones sobre Kurt Gödel,* Alianza, Madrid.

LAS MATEMÁTICAS DE LA SEGURIDAD

S. González y C. Martínez
Departamento de Matemáticas
Universidad de Oviedo

ARBOR Ciencia, Pensamiento y Cultura
CLXXXIII 725 mayo-junio (2007) 419-425 ISSN: 0210-1963

ABSTRACT: *The aim of this paper is to show the important role that Mathematics play in the Information theory. It has been intended for non specialists, drawing a general picture of the present situation.*

KEY WORDS: *Error correcting codes, cryptography, digital information, public key, secret key.*

RESUMEN: El objetivo del trabajo es mostrar el papel esencial que juegan actualmente las matemáticas en la teoría de la información. El trabajo está pensado para no especialistas y pretende dibujar en unas breves pinceladas como es la situación actual.

PALABRAS CLAVE: Códigos correctores de errores, criptografía, información digital, clave pública, clave secreta.

1. Introducción

La información, tanto por la cantidad como por la velocidad con la que circula, se ha convertido en una seña de identidad del momento actual. El trabajo de Shannon, en el que se da carácter matemático a la información, convirtiéndola en algo que se puede medir y tratar de modo científico, representó, sin lugar a dudas, un punto de inflexión en la teoría de la información. Hoy en día nadie duda de que la información es poder y como tal, un bien valioso que tiene que ser protegido de ataques a su integridad o a su confidencialidad.

Si lo pensamos detenidamente, la cantidad de información, en muchos casos información muy sensible, que circula actualmente por canales más o menos públicos, puede hacernos sentir vértigo. La mayoría de nosotros entra de modo habitual en Internet y sabe que se puede encontrar información sobre prácticamente todo, si uno sabe buscarla. Tambien estamos acostumbrados a intercambiar información con nuestro banco, con una agencia de viajes o realizando compras a través de la red. Es claro que todos nosotros deseamos tener la seguridad de que la información que enviamos sólo es accesible para su legítimo receptor y que no cae en "manos indebidas".

La seguridad de la información ha pasado de ser exclusividad de la Política, la Diplomacia, los Servicios de Inteligencia o las Altas Finanzas, a convertirse en algo cotidiano, que en mayor o menor medida nos afecta a todos y cada uno de nosotros.

Parece claro que la información tiene que ser protegida, tanto en los aspectos de fidelidad de la información, detectando y corrigiendo los posibles errores generados por el ruido (nombre genérico para todas las perturbaciones eléctricas, magnéticas o de cualquier tipo que afecten al canal por el que se transmite la información) como en el aspecto de confidencialidad e integridad de la misma. Y en este punto las Matemáticas juegan un papel de extraordinaria importancia. Siguiendo a N. Koblitz podemos decir que: "La enorme utilidad de las matemáticas en la seguridad de la información está bordeando el misterio y no existe explicación racional para ella", parafraseando a Eugene Wigner que escribió esa afirmación en relación al papel jugado por las matemáticas en las Ciencias Naturales y especialmente en Física.

2. Corrección de errores

Cuando hablamos de información siempre tenemos en mente información digital, secuencias de ceros y unos, que pueden ser transmitidos por un canal. La información de un periódico o de una fotografía no es digital, pero se puede transformar en información digital y por eso podemos leer el periódico por internet o enviar fotografías por correo electrónico. Los códigos se inventaron para corregir los errores que se producen en la comunicación a través de canales con ruido. Tratan de reproducir lo que hacemos en la vida cotidiana cuando estamos hablando y un ruido ambiental nos impide entender lo que nos ha dicho nuestro interlocutor. Le pedimos que nos repita lo que ha dicho. Por eso el primer paso es la detección de los errores en la información recibida. Pero no siempre podemos solicitar que nos reenvíen la información que ha llegado defectuosa. Aparte del coste que tiene el uso del canal, puede ser inviable. Pensemos en información almacenada en un disco y que se abre al cabo de un tiempo, cuando ya no se puede pensar en su reenvio. O en una fotografía enviada por un satélite espacial desde una posición concreta. La idea es sencilla. Se añade a la información que se quiere enviar una serie de dígitos (de control) que no contienen información, pero permiten detectar y, eventualmente corregir, errores, siempre que el número de errores producidos no exceda la capacidad correctora del código. Los códigos correctores forman parte de nuestra vida cotidiana, como ocurre con la letra que se añade al DNI o el ISBN de los libros. También lo utiliza la naturaleza en el código genético, aunque no sepamos exactamente como funciona.

En el diseño de códigos correctores de errores cuyo almacenamiento no desborde las capacidades de nuestro ordenador, las matemáticas juegan un papel decisivo. Todos los códigos considerados de modo usual son códigos lineales, es decir, disponemos de todas las herramientas del álgebra lineal. Pero no son las únicas. Teoría de cuerpos finitos, polinomios sobre ellos, geometría algebraica o matemática discreta (diseños, geometrías finitas, etc.), teoría de anillos, son algunas de las partes de las matemáticas que juegan un papel importante en la teoría de códigos correctores de errores. Dado que en general no existen algoritmos eficientes para la descodificación de un código lineal, el diseño de códigos con buenas propiedades, es decir con algoritmos de descodificación eficientes, sigue siendo un campo abierto al trabajo y la imaginación de los matemáticos, que pueden aplicar las técnicas y herramientas que les son familiares; probablemente en algunos casos de modo sorprendente.

3. Seguridad

Pero nuestro objetivo es poner de relieve el papel que juegan las matemáticas en la seguridad de la información.

La protección de la información, o más concretamente de cierto tipo de información, ha sido una preocupación de la humanidad desde tiempos remotos. Todos hemos oido hablar del cifrado usado por César para enviar sus mensajes o del escítalo de los lacedemonios. En algunos casos los procesos de cifrado fueron especialmente eficaces. Pensemos en los jeroglíficos usados por los sacerdotes egipcios, que no fueron descifrados hasta el siglo XIX. Todos estos cifrados, usados desde la antigüedad corresponden a lo que hoy llamamos criptografía de clave privada o simétrica. El texto se enmascara, transformándolo en un texto cifrado, usando para ello una clave que debe permanecer secreta y debe ser conocida sólamente por el remitente (o emisor) del mensaje y su legítimo receptor, que básicamente utiliza la misma clave para recuperar el mensaje original, o en todo caso, el coste computacional de cifrar y descifrar un mensaje es el mismo.

La auténtica revolución que cambió el panorama de la criptografía se produjo en el año 74, con el artículo en el que Diffe y Hellman introducen la criptografía de clave pública. La idea base es que la clave de cifrado de un determinado usuario A sea pública y cualquier otro usuario de la red le pueda enviar mensajes cifrados a A usando dicha clave pública. Pero sólo A, que tiene la clave privada, será capaz de descifrar los mensajes cifrados. ¿Cómo es posible que cualquier usuario pueda cifrar mensajes y no pueda descifrarlos? Es en este punto dónde las matemáticas juegan un papel esencial. La existencia de criptografía de clave pública se basa en la existencia de funciones de una vía.

Una función de una vía es una función para la cual es fácil calcular la imagen de cualquier elemento, pero la determinación de la imagen inversa de un elemento, aún sabiendo que exista, es muy costoso computacionalmente, de hecho inasumible.

ARBOR CLXXXIII 725 mayo-junio [2007] 419-425 ISSN: 0210-1963

Los criptosistemas de clave pública más usuales se basan en el problema de la factorización (RSA) y en el problema del logaritmo discreto. Dados dos números primos, aunque sean muy grandes, se pueden multiplicar sin problemas, pero factorizar un número grande (pensemos en números de 200 cifras decimales), aún sabiendo que es compuesto, es extremadamente costoso y requiere un tiempo que no lo hace factible. Para diseñar un esquema RSA el usuario debe elegir dos primos grandes p y q (para garantizar la seguridad p y q deben cumplir algunas propiedades adicionales) y un cierto entero e, que también veremos debe cumplir alguna condición. Su clave pública será el par (N, e) dónde $N = pq$. De este modo, los mensajes, que se identifican previamente con clases de restos módulo N (o si se quiere con enteros positivos menores que N), se cifran haciendo una exponenciación modular. Es decir, el cifrado de un mensaje m es el resto de dividir m^e entre N. Notemos que para descifrar necesitariamos hallar la inversa de la exponenciación anterior módulo N, lo que en general no se puede hacer si no se dispone de una información adicional, de la que dispone el propietario de la clave y que debe evitar llegue a ser conocida. En este caso dicha información adicional es el par de números primos p y q en los que se factoriza N.

Dado un entero n mayor que 1, se llama función de Euler de n, $\phi(n)$, al número de enteros positivos, menores que n y relativamente primos con n. Si tratamos de calcular la función de Euler de un número grande n, el procedimiento es muy costoso computacionalmente, comparable al coste de factorizar el número n. Pero si conocemos *a priori* la factorización de n, entonces es inmediato calcular $\phi(n)$. En nuestro caso, si $N = pq$, entonces $\phi(N) = (p - 1)(q - 1)$. Tambien probó Euler (del que se conmemora este año el 300 aniversario de su nacimiento) que si a es un entero relativamente primo con N, entonces la potencia $\phi(N)$ de a es congruente con 1 módulo N ($a^{\phi(N)} \equiv 1 \bmod N$). Si elegimos el entero e relativamente primo con $\phi(N)$, entonces podemos encontrar muy fácilmente, usando el algoritmo euclídeo de la división, otro entero d tal que $ed \equiv 1 \bmod \phi(N)$. Ahora para el propietario de la clave es muy fácil descifrar. Para recuperar el mensaje m cuyo texto cifrado es c ($c \equiv m^e \bmod N$) sólo tiene que hacer una nueva exponenciación, $m \equiv c^d \bmod N$.

Son resultados de teoría de números los que suministran la función de una vía en la que se sustenta la seguridad del RSA.

Otra función de una vía viene asociada al problema del logaritmo discreto. Si $G = < g >$ es un grupo cíclico convenientemente elegido, es computacionalmente imposible encontrar, para un elemento arbitrario y del grupo, el exponente x tal que $y = g^x$. Tal exponente x se llama el logaritmo discreto de y en base g. En particular se sabe que ese es el caso si tomamos como grupo cíclico el grupo multiplicativo de los elementos no nulos de un cuerpo finito (suficientemente grande) o el grupo asociado a una *buena* curva elíptica.

En este caso, si un usuario A quiere diseñar un criptosistema de clave pública tipo ElGamal, selecciona un adecuado grupo cíclico $G = < g >$, que hace público al igual que el generador del mismo y también hace público un elemento del grupo, y con $y = g^k$, siendo k un número adecuado que debe mantener secreto, difícil de determinar para cualquier otro usuario y que permitirá a A descifrar los mensajes que le envian. Notemos que k es el logaritmo discreto de y en base g, luego la seguridad del sistema se basa en que sea computacionalmente imposible calcularlo. Ahora los mensajes se identifican de algún modo con elementos del grupo. Para cifrar el mensaje m, otro usuario B determina aleatoriamente un r y envia el par (g^r, my^r). Para descifrar el mensaje, A considera la primera componente del par, g^r y la eleva a su clave privada k. Como $(g^r)^k = (g^k)^r = y^r$, para recuperar el mensaje m basta que divida la segunda componente del par recibido por el elemento $(g^r)^k$ que acaba de calcular. Notemos que r tambien debe elegirse de modo adecuado, pues un tercer usuario podría recuperar el mensaje concreto m si es capaz de determinar r que es el logaritmo discreto en base g de la primera componente del mensaje cifrado.

4. Otros tipos de criptografía

Hay otras muchas partes de las matemáticas que tienen aplicaciones en Criptografía. Por ejemplo la Combinatoria. En el año 78 se recibió con entusiasmo una propuesta de Hellman y Merkle de un criptosistema basado en el problema de la mochila. El problema de la mochila consiste en, dada una sucesión de números $\{b_1, ..., b_n\}$ y un número S (menor o igual que la suma de los términos de la sucesión) determinar si es posible encontrar algunos términos de la sucesión cuya suma

nos dé el número *S*. Se sabe que en general es un problema difícil y no existe ningún algoritmo eficiente para resolverlo (en términos de teoría de la complejidad es un problema NP-completo). Pero existe un caso en el que el problema es especialmente sencillo de resolver, las llamadas sucesiones supercrecientes, en que cada término es mayor que la suma de los que le preceden. Por ello se parte de una sucesión supercreciente, que forma parte de la clave secreta, y se enmascara con una serie de operaciones algebraicas, que tambien deben mantenerse secretas, para transformarla en una sucesión aparentemente arbitraria y sin "buenas propiedades", que es la clave pública. El recuperar el mensaje enviado a partir de su texto cifrado obligaría a un usuario no autorizado a resolver el problema de la mochila en un caso difícil, mientras que el propietario de la clave lo transforma, deshaciendo las operaciones algebraicas de su clave secreta, en un problema de la mochila en el caso sencillo de sucesiones supercrecientes, para las cuales existe un algoritmo muy eficaz.

Este esquema de cifrado y descifrado era muy eficiente, unas 100 veces más rápido que el RSA. Pero en 1984 Shamir, uno de los padres del RSA, rompió completamente el criptosistema, sin recuperar la clave secreta, sino encontrando nuevos elementos que jugaban un papel análogo y le permitian recuperar el mensaje en claro sin conocer la clave secreta. Aunque se intentó salvar el criptosistema, introduciendo iteraciones y modificaciones, todas ellas fueron rotas por Shamir. Durante un tiempo se consideró que la criptografía basada en problemas combinatorios no tenia futuro, a pesar de la existencia de muchos problemas NP-completos conocidos que serian los candidatos naturales para definir una función de una vía. No obstante hoy en día se ha recuperado la idea de utilizar problemas de combinatoria y se está produciendo una notable actividad en esta dirección, si bien no hay todavía ninguna propuesta concreta que sea viable y eficaz.

La aparición de los ordenadores cuánticos supondria una amenaza letal para los sistemas criptográficos de clave pública más utilizados (basados en factorización y en el problema del logaritmos discreto), dado que el proceso de multiplicar dos números y la factorización de un número pasarian a ser problemas de complejidad similar con un ordenador cuántico. Por ello se han buscado primitivas criptográficas basadas en otros aspectos matemáticos, con problemas en los que un ordenador cuántico no supondría un cambio sensible. Una de las ramas que ha jugado y juega un papel fundamental es la teoría de grupos, tanto finitos como infinitos.

En general los grupos infinitos considerados en criptografía son finitamente presentados, es decir admiten un conjunto de generadores finito que satisfacen un conjunto finito de relaciones. Los esquemas propuestos se basan en la conocida dificultad de dos problemas, el de la palabra (¿podemos determinar si una palabra en los generadores representa o no el elemento identidad en el grupo?) y el de la conjugación (determinar si dos elementos del grupo son o no conjugados en el grupo).

En el caso de grupos finitos en general las propuestas se basan en la existencia de ciertos conjuntos, con propiedades especiales, que permiten escribir todos los elementos del grupo como producto de elementos de dichos conjuntos (como signaturas logarítmicas, mallas o cubiertas, ver [15]).

También se han utilizado grupos Braid en criptografía, si bien los esquemas diseñados han sido criptoanalizados en la mayoría de los casos.

Finalmente, en este sentido, comentemos que la primera propuesta de diseño para un criptosistema IND-CCA (que se ha convertido actualmente en la noción standard de seguridad deseable), se debe a Cramer y Shoup tomando como base grupos abelianos. También se han presentado propuestas basadas en grupos no abelianos (ver [16]).

5. Criptoanálisis

Las exigencias de seguridad han ido cambiando, dependiendo de necesidades y del perfeccionamiento y la sistematización lograda por el criptoanálisis. Se han desarrollado diversas nociones de seguridad, siendo este un campo teórico de trabajo en el que aún queda mucho por hacer. La noción de seguridad considerada depende de la cantidad de información conocida por un adversario y el tipo de ataques que pueda llevar a cabo. En algunos casos el adversario conoce pares de texto y sus cifrados, pero en otros casos puede ob-

tener el cifrado de cualquier mensaje previamente elegido, como ocurre en la criptografía de clave pública. Tambien puede ocurrir que cuando el atacante trata de recuperar un mensaje concreto *m* a partir de su cifrado *c,* tenga acceso al descifrado de cualquier otro texto cifrado.

El criptoanálisis y la criptografía van íntimamente ligados. Antes de proponer un sitema de cifrado, es necesario hacer una tarea de criptoanálisis, para tener una mínima seguridad de la robustez del esquema. El criptoanalista, en su tarea de buscar vulnerabilidades de los esquemas propuestos, utiliza gran variedad de herramientas matemáticas: técnicas estadísticas, algebraicas, algoritmos de optimización, teoría de números, etc. Una de las técnicas más potentes utilizadas por el criptoanálisis está basada en retículos.

Un retículo es el conjunto de combinaciones lineales enteras de un conjunto de vectores linealmente independientes (su estructura en dimensión 2 ó 3 se parece a una red). Estas estructuras tienen aplicaciones en otras partes de las matemáticas, como álgebras de Lie, en teoría de códigos correctores o en otras ciencias, como la cristalografía.

Las aplicaciones a criptología se hacen a través de la resolución de ciertos problemas como el del vector más corto. La complejidad de los mejores algoritmos conocidos para resolverlos crecen, al menos en el peor de los casos, exponencialmente con la dimensión del retículo.

Sin embargo A. J. Lenstra, H. W. Lenstra y L. Lovász vieron que si se quiere encontrar un vector *relativamente corto,* el problema es mucho más fácil y diseñaron un algoritmo, el LLL, que lo resuelve en un tiempo de ejecución que es polinomial en la dimensión del retículo.

El algoritmo LLL se utilizó en el problema de la mochila y en el criptoanálisis al sistema mencionado propuesto por Merkle y Hellman y también para probar la debilidad de algunas funciones hash (que juegan un importante papel en criptografía) o la vulnerabilidad de algunos generadores pseudoaleatorios de números.

Aunque la aplicación más espectacular de los retículos ha sido en criptoanálisis, también se han aplicado en criptografía. Ajtai y Dwork propusieron un criptosistema de clave pública basado en una variante, tambien difícil, del problema del vector más corto y además la seguridad se basaba en la difícultad de resolver el problema en un caso cualquiera, no en uno especialmente desfavorable. Pero si el tamaño de las claves es grande, el criptosistema es ineficiente y si se reducen las claves, el criptosistema es, a pesar de todo, vulnerable.

Goldwaser, Goldreich y Halevi propusieron otro criptosistema de clave pública cuya seguridad dependia de otro problema difícil, el encontrar el vector de un reticulo más cercano a otro vector dado. Este algoritmo es más eficiente que el de Ajtai y Dwork, pero la forma especial de los retículos utilizados los hace vulnerables ante un cierto tipo de ataques.

En la actualidad sólo existe un criptosistema de clave pública en uso que se basa en retículos, si bien no en su descripción inicial. El ataque más fuerte conocido se basa en resolver el problema del vector más corto en un retículo que se construye a partir de la clave pública y que no consigue resolverse porque se pueden utilizar dimensiones grandes debido a la eficiencia del sistema. Hay que hacer notar, sin embargo, que no hay ninguna demostración de que atacar al sistema pase necesariamente por resolver el problema del vector más corto.

Coppersmith realizó un significativo avance en el campo del criptoanálisis al publicar en 1996 unos algoritmos basados en retículos que permitian encontrar, con complejidad polinómica, soluciones pequeñas de ecuaciones enteras. Una versión modificada y más operativa dada por Howgrave-Graham permitió encontrar soluciones pequeñas de ecuaciones modulares. El diseño por parte de Boneh y Durfee de un algoritmo para atacar el RSA cuando la clave privada se escoge demasiado pequeña ha sido, probablemente, la aplicación más importante.

Finalmente notemos que en ocasiones herramientas del criptoanáliss se utilizan para probar la seguridad de un sistema criptográfico. Es el caso de un algoritmo de Coppersmith que busca raíces pequeñas de ecuaciones enteras en dos variables y que fue utilizado por May para probar que, en ciertas condiciones, la seguridad del RSA es equivalente al problema de la factorización.

6. Conclusiones

No se debe deducir de lo anterior, que la criptología se reduce al diseño de criptosistemas y al posterior estudio de sus debilidades en el criptoanálisis. Los problemas de los que se ocupa la criptografía son muy numerosos y no podríamos enumerarlos en estas páginas. Aparte del uso de passwords, ya generalizado, y todo lo que rodea al comercio y dinero electrónico, mencionaremos, a modo de ejemplo, sólo algunos de ellos:

1. *Autenticación de mensaje y firma digital:* Se trata de una de las principales aplicaciones de la criptografía de clave pública, aunque en muchas ocasiones se combine con clave privada. La firma digital, a diferencia de la manuscrita, garantiza no sólo que el emisor es quien afirma ser, sino que el mensaje llega a su destinatario sin alteraciones o modificaciones en el mismo.
2. *Compartición de secretos:* Se quiere dar información a un grupo de gente de modo que una información secreta sea recuperada si cualquier subconjunto de k personas colabora, pero no se consiga si son sólamente $k - 1$ los que colaboran.
3. *Acuerdo de bit:* Reproduce el proceso de lanzamiento de una moneda entre dos personas que están a distancia y tienen que interactuar de modo secuencial y no en el mismo instante.
4. *Pruebas de conocimiento cero y transferencia olvidadiza (oblivious transfer):* Se utiliza cuando una persona quiere convencer a otra de que posee una información o es capaz de hacer algo (por ejemplo demostrar un teorema) sin revelar los detalles. Un modo de construir pruebas de conocimiento cero no interactivas es a través de un canal de transferencia olvidadiza, que es un sistema para enviar dos paquetes de información cifrada sabiendo emisor y receptor que sólo uno de los dos paquetes puede ser descifrado y leido por el receptor y el emisor ignora cual de los dos paquetes será el que puede leer el receptor.

A los anteriores problemas podemos añadir el descubrimiento parcial de secretos, la venta de secretos, esquema electoral, transferencia inconsciente, firma de contratos, correo con acuse de recibo, etc. Como vemos la lista se prolonga de un modo realmente impresionante y la actividad en el campo es incesante. Basta echar un vistazo a las actas de alguna de las importantes reuniones que se celebran anualmente en el ámbito internacional, por ejemplo las del último Eurocyrpt en San Petersburgo (el de este año será en Barcelona) o a las de TCC 2007 (Theory of Cryptography Conference) que se celebrará este febrero en Amsterdam para ver la cantidad de investigación que se está realizando.

Hemos tratado de reflejar como distintas partes de las Matemáticas han jugado y están llamadas a jugar un papel esencial en el desarrollo de la Criptografia, especialmente en Clave Pública. Por supuesto la seguridad de la información necesita profesionales de muchos ámbitos, y muy especialmente informáticos. Shafi Goldwasser publicó un artículo en los Proceedings del IEEE en 1997 con el título: "Nuevas direcciones en Criptografía, Veinte años más tarde", en alusión a los 20 años transcurridos desde la introducción de la Criptografía de clave pública. El subtítulo de dicho artículo es "Criptografía y Teoría de la Complejidad: un emparejamiento hecho en el cielo". Esta idea aparece también expresada por Koblitz, que plantea la importancia de propuestas en criptografía, aunque no sean prácticas ni aplicables eventualmente. Las cuatro razones esgrimidas para ello son:

1. Pueden dar origen a nuevas cuestiones matemáticas o generar nuevos puntos de vista sobre teorías anteriores.
2. Pueden sugerir nuevas líneas de investigación en aspectos teóricos de Ciencias de la Computación y arrojar luz sobre las interrelaciones entre clases de complejidad.
3. Pueden ser un medio de popularizar matemáticas y Ciencias de la computación.
4. Pueden ser un medio efectivo para la enseñanza a niveles no-universitarios.

Por tanto los matemáticos han jugado y están llamados a jugar un importante papel en la seguridad de la información. Y al mismo tiempo, la fructífera relación con Ciencias de la Computación debe ser cuidada, mantenida y estimulada.

Referencias

[1] M. Ajtai y C. Dwork, A public-key cryptosystem with worst-case/ average case equivalente. *Proc. of 29th STOC, ACM.* 1997, 284-293.

[2] M. Bellare, A. Desai, D. Pointcheval y P. Rogaway, Relations Among Notions of Security for Public-Key Encryption Schemes *Proc. of CRYPTO '98, LNCS 1462,* 1998, 26-45.

[3] D. Boneh y G. Durfee, Cryptanalysis of RSA with private key less than $n^{0,292}$, *Proc. of Eurcrypt'99, Lecture Notes in Computer Science 8494*, 1999, 1-11.

[4] I. Cascudo, Aplicaciones de Retículos en Criptología. *Tesina de Licenciatura, Universidad de Oviedo,* 2006.

[5] D. Copperstmith, Small solutions to polynomial equations and low exponent RSA vulnerabilities. *Journal o f Cryptology 10(4),* 1997, 233-260.

[6] D. Copperstmith, Finding small solutions to small degree polynomials. *Proc. of Cryptography and Lattices Conference'01, Lecture Notes in Computer Science 2146,* 2001.

[7] D. Copperstmith y A. Shamir, Lattice attacks on NTRU. *Proc. of Eurocrypt'97, Lecture Notes in Computer Science 1238,* 1997, 52-61.

[8] R. Cramer y V. Shoup, A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack *Proc. of CRYPTO'98. LNCS, vol. 1162.,* 1999, 13-25.

[9] R. Cramer y V. Shoup, Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption *Cryptology e Print Archive: Report 2001/085,* 2001, 1-62.

[10] W. Diffie y M. E. Hellman, New directions in Cryptology. *IEEE Trans. Information Theory 22,* 1976, 644-654.

[11] O. Goldreich, S. Goldwasser y S. Halevi, Public-key cryptosystems from lattice reduction problems. *Proc. of Crypto'97, Lecture Notes in COmputer Science 1294,* 1997, 112-131.

[12] O. Goldreich. S. Goldwasser y S. Halevi, On the limits of non-approximitability of lattice problems. *Proc. of 80th STOC, ACM,* 1998.

[13] S. Golwasser, New directions in Cryptography: Twenty some years latter (or a Match Made in Heaven), *Proc. o f the 88th Annual IEEE Symposium on Foundations of Competer Science, FOCS'97,* 1997, 314-324.

[14] S. González, M. I. González-Vasco y C. Martínez, Esquemas de cifrado basados en grupos: pasado y futuro CD: *Tendencias actuales en la Criptología, Sesión especial de MAT.es 2005* ISBN: 84-689-0117-2.

[15] M. I. González-Vasco. Criptosistemas basados en Teoría de grupos. *Tesis Doctoral, Universidad de Oviedo,* 2000.

[16] M. I. González Vasco, C. Martínez, R. Steinwandt y J. L. Villar, A new CramerShoup like methodology for group based probably secure schemes. *Lecture Notes in Computer Science, Theory of Cryptography 3378,* 2005, 495-509.

[17] A. J. Lenstra, H.W. Lenstra y L. Lovász, Factoring polynomials with rational coefficients. *Mathematische Annalen 261.* 1982, 513-534.

[18] N. Koblitz, *Adgebraic Aspects of Cryptography,* Springer 2004.

[19] R. Merkle y M. Hellman, Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions of Information Theory, IT-24(5),* 1978, 525-530.

[20] P. Q. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem. *Lecture Notes in Computer Science 1666,* 1999, 288-304.

[21] P. Q. Nguyen y J. Stern, Lattice reduction in cryptology: An update. *Lecture Notes ira COmputer Science 1838,* 2000, 85-112.

[22] P. Q. Nguyen y J. Stern, The two faces of lattice in cryptography. *Lecture Notes in Computer Science 2146,* 2001.

[23] C. E. Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J. 18,* 1949, 656-715.

Recibido: 15 de enero de 2007
Aceptado: 25 de enero de 2007